(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 853 288 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
15.07.1998 Bulletin 1998/29

(51) Int. Cl.^{6}: **G06K 7/10**, G01S 13/82

(21) Application number: 97310181.9

(22) Date of filing: 16.12.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 31.12.1996 US 777832

(71) Applicant:
LUCENT TECHNOLOGIES INC.
Murray Hill, New Jersey 07974-0636 (US)

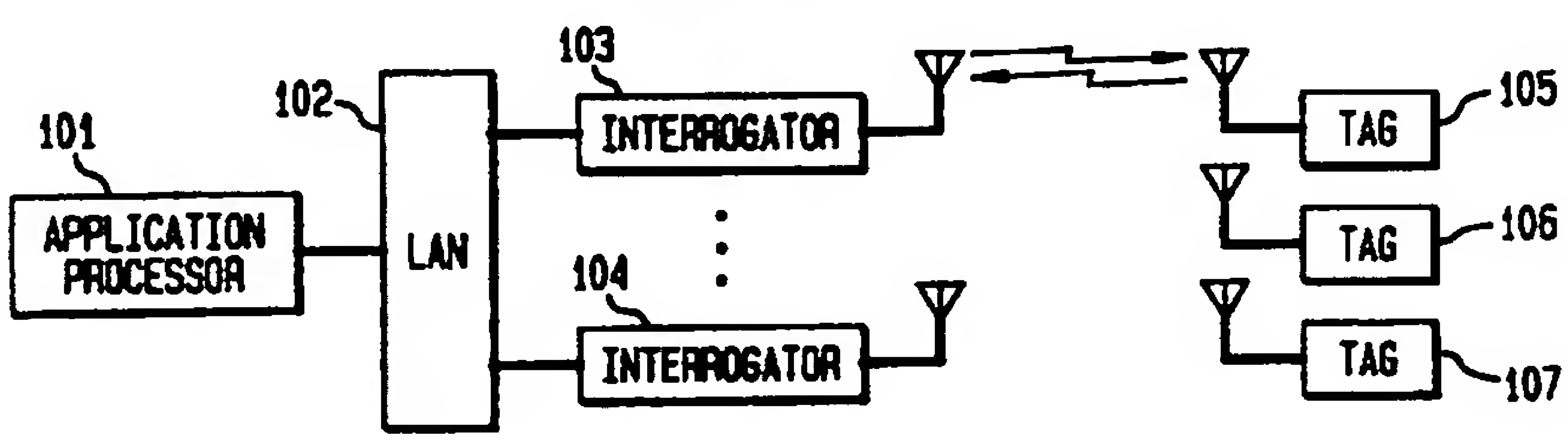
(72) Inventors:
- MacLellan, John Austin
Freehold, New Jersey 07728 (US)
- Vannucci, Giovanni
Red Bank, New Jersey 07701 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) **Encryption for modulated backscatter systems**

(57) The present invention enables a Tag and Interrogator to exchange proprietary information using Modulated BackScatter (MBS) technology. This invention discloses a method for encrypting the RFID user's PIN and thereby making the interception and the subsequent illegal use of RFID accounts at least as difficult as a present day ATM cards. For example, the encryption method can be based upon the US Digital Encryption Standard (DES), either first or third level. The Tag's personal encryption key is only known by the financial database and the RFID Tag. This method can be applied to any type of financial, debt, identification, or credit card.

FIG. 1



EP 0 853 288 A2

Description

Field of the Invention

This invention relates to wireless communication systems and, more particularly, to a wireless communication system which uses digital encryption encoding to ensure secure transmission of private information using modulated backscatter technology.

Related Applications

START Related subject matter is disclosed in the following U.S. patent applications assigned to the Assignee hereof: U.S. patent application Ser. No. 08/571004, filed December 12, 1995, by MacLellan et al. and entitled "Enhanced Uplink Modulated Backscattering System;" U.S. patent application Ser. No. 08/492174, filed June 19, 1995, by MacLellan et al. and entitled "Full Duplex Modulated Backscattering System;" and U.S. patent application Ser. No. 08/492173, filed June 19, 1995, by Shober et al. and entitled "Dual Mode Modulated Backscatter System." END Related subject matter is disclosed in the following applications filed concurrently herewith and assigned to the same Assignee hereof: U.S. patent applications "Shielding Technology In Modulated Backscatter System," Serial No. ________; "QPSK Modulated Backscatter System," Serial No. ________; "Modulated Backscatter Location System," Serial No. ________; "Antenna Array In An RFID System," Serial No. ________; "Subcarrier Fluency Division Multiplexing Of Modulated Backscatter Signals," Serial No. ________; "IQ Combiner Technology In Modulated Backscatter System," Serial No. ________; "In-Building Personal Pager And Identifier," Serial No. ________; "In-Building Modulated Backscatter System," Serial No. ________; "Inexpensive Modulated Backscatter Reflector," Serial No. ________; "Passenger, Baggage, And Cargo Reconciliation System," Serial No. ________. Related subject matter is also disclosed in the following applications assigned to the same assignee hereof: U.S. patent application 08/504188, entitled "Modulated Backscatter Communications System Having An Extended Range"; U.S. Patent Application Serial No 08/492,173, entitled "Dual Mode Modulated Backscatter System,"; U.S. Patent Application Serial No. 08/492,174, entitled "Full Duplex Modulated Backscatter System,"; and U.S. Patent Application Serial No. 08/571,004, entitled "Enhanced Uplink Modulated Backscatter System."

Background of the Invention

Radio Frequency IDentification (RFID) systems are used for identification and/or tracking of equipment, inventory, or living things. RFID systems are radio communication systems that communicate between a radio transceiver, called an Interrogator, and a number of inexpensive devices called Tags. In RFID systems, the Interrogator communicates to the Tags using modulated radio signals, and the Tags respond with modulated radio signals. The Interrogator first transmits an amplitude modulated signal to the Tag. Then, the Interrogator transmits a Continuous-Wave (CW) radio signal to the Tag. The Tag then modulates the CW signal, using Modulated BackScattering (MBS), where the antenna is electrically switched, by the Tag's modulating signal, from being an absorber of RF radiation to being a reflector of RF radiation; thereby encoding the Tag's information onto the CW radio signal. The Interrogator demodulates the incoming modulated radio signal and decodes the Tag's information message.

Over the next decade an enormous growth in the number and proliferation of RFID applications is expected. Many emerging applications will be of a financial nature and will require, for example, that a user's Personal Identification Number (PIN) cannot be intercepted by a hostile eavesdropper. The cellular phone industry is presently under siege by network pirates and industry losses are quoted to be approaching one billion dollars annually. So as not to repeat this particular failing of the cellular industry, RFID system designers should consider network security a top priority. There are three major security issues when transferring data in a wireless system:

1. A legitimate Tag and a legitimate Interrogator are involved in a communication session transferring sensitive data that a hostile eavesdropper would like to intercept.
2. A legitimate Interrogator would be queried by a fraudulent Tag trying to obtain service, such as to acquire data stored in the network or in an Application Processor. (This is similar to the case of someone stealing cellular air time.)
3. A legitimate Tag would be queried by a fraudulent Interrogator trying to acquire data stored in the Tag's memory (like stealing the PIN number from a cellular telephone).

This invention discloses a method for encrypting both the data in a Tag's memory and the data stored in an Application Processor, where by transferring only ciphered data between network endpoints, one can thwart all three security breaches outlined above. This method encrypts the RFID user's PIN and therefore makes the interception and the subsequent illegal use of RFID data at least as difficult as for present day ATM cards. The encryption method can be based upon the US Digital Encryption Standard (DES), either first or third level. The Tag's personal encryption key is only known by the financial database and the RFID Tag. This method can be applied to any type of financial, debt, identification or credit card.

Summary of the Invention

In accordance with the present invention, a MBS radio communication system comprises an Interrogator which generates a first modulated signal by modulating a first information signal onto a radio carrier signal. The Interrogator transmits the first modulated signal to at least one remote Tag of the system. The remote Tag receives and processes the received first modulated signal. A second information signal backscatter-modulates the reflection of the first modulated signal, the reflected signal being a second modulated signal. The Interrogator receives and demodulates the second modulated signal to obtain the second information signal. In one embodiment, demodulation utilizes a homodyne detector and the first modulated signal as the local oscillator source for the homodyne detector. In another embodiment, the second information signal is modulated onto a subcarrier, which is then backscatter-modulated onto the first modulated signal. The Interrogator communicates the second information signal to an Application Processor; the second information signal contains private information known only to the Tag and to the Application Processor. Both the Tag and Application Processor use digital encryption techniques to cipher the end-to-end communications of the private information.

The present disclosure outlines three levels of security for which, depending on the RFID application, an Application Processor, at least one Interrogator, and at least one Tag can exchange information: The first level is the "Normal" mode, where a Tag and Interrogator exchange the RFID of the Tag. The second level is to transmit and detect a "secure" RFID between a Tag and Application Processor, using the Interrogator as a "wireless-to-wiredline" converter. The third level is the transfer of secure messages between a Tag and Application Processor. This can include downloading new information to a Tag; this is a "Read/Write" Tag where the data stored in memory is sensitive, i.e., cash stored on a debit card.

Brief Description of the Drawing

In the drawing,

FIG. 1 shows a block diagram of an illustrative Radio Frequency Identification (RFID) system;
FIG. 2 shows a block diagram of an illustrative Interrogator Unit used in the RFID system of FIG. 1;
FIG. 3 shows a block diagram of a Tag Unit used in the RFID system of FIG. 1;
FIG. 4 shows the flow of information between the Tag, Interrogator and the Application Processor vs. time during a secure message transfer;
FIG. 5 shows a block diagram of how a Tag's processor and the Application Processor processor calculate the random query response;
FIG. 6 shows the flow of information between the Applications Processor, the Interrogator, and at least one Tag, where the Applications Processor is writing new information to the Tag's memory.

Detailed Description

One class of RFID applications involves using RFID technology to read information from a Tag affixed to a container or pallet. In this application, the container is moved across the reading field of an Interrogator. The reading field is defined as that volume of space within which a successful transaction can take place. While the Tag is in the reading field, the Interrogator and Tag must complete their information exchange before the Tag moves out of the Interrogation field. Since the Tag is moving through the reading field, the RFID system has only a limited amount of time to successfully complete the transaction.

Normal Mode

With reference to FIG. 1, there is shown an overall block diagram of an illustrative RFID system useful for describing the application of the present invention. An Application Processor 101 communicates over Local Area Network (LAN) 102 to a plurality of Interrogators 103-104. The Application Processor and the Interrogator functions may be present in the same device, or separate. In this disclosure we refer to the logical functions performed by each device. The Interrogators may then each communicate with one or more of the Tags 105-107. For example, the Interrogator 103 receives an information signal, typically from an Application Processor 101. The Interrogator 103 takes this information signal and Processor 200 (FIG. 2) properly formats a downlink message (Information Signal 200a) to be sent to the Tag. With joint reference to FIGS. 1 and 2, Radio Signal Source 201 generates a radio signal, the Modulator 202 modulates the Information Signal 200a onto the radio signal, and the Transmitter 203 sends this modulated signal via Antenna 204, illustratively using amplitude modulation, to a Tag. The reason amplitude modulation is a common choice is that the Tag can demodulate such a signal with a single, inexpensive nonlinear device (such as a diode).

In the Tag 105 (see FIG. 3), the Antenna 301 (frequently a loop or patch antenna) receives the modulated signal. This signal is demodulated, directly to baseband, using the Detector/Modulator 302, which, illustratively, could be a single Schottky diode. The diode should be appropriately biased with the proper current level in order to match the impedance of the diode and the Antenna 301 such that losses of the radio signal are minimized. The result of the diode detector is essentially a demodulation of the incoming signal directly to baseband. The Information Signal 200a is then amplified, by Amplifier 303, and synchronization

recovered in Clock and Frame Recovery Circuit 304. The Clock Recovery Circuit 304 can be enhanced by having the Interrogator send the amplitude modulated signal using Manchester encoding. The resulting information is sent to a Processor 305. The Processor 305 is typically an inexpensive 8-bit microprocessor; the Clock Recovery Circuit 304 can be implemented in a ASIC (Application Specific Integrated Circuit) which works together with Processor 305. The Processor 305 generates an Information Signal 306 to be sent from the Tag 105 back to the Interrogator (such as Interrogator 103). This Information Signal 306 (under control of Clock Recovery and Frame synchronization 304) is sent to a Modulator Control Circuit 307, which uses the Information Signal 306 to modulate a subcarrier frequency generated by the subcarrier Frequency Source 308. The Frequency Source 308 could be a crystal oscillator separate from the Processor 305, or it could be a frequency source derived from signals present inside the Processor 305, such a a divisor of the primary clock frequency of the Processor. The Modulated Subcarrier Signal 311 is used by Detector/Modulator 302 to modulate the modulated signal received from Tag 105 to produce a modulated backscatter signal, also referred to herein as a reflected signal. This is accomplished by switching on and off the Schottky diode using the Modulated Subcarrier Signal 311, thereby changing the reflectance of Antenna 301. A Battery 310 or other power supply provides power to the circuitry of Tag 105.

Secure Mode

The present invention enables a Tag and Interrogator to exchange proprietary information using MBS technology. FIG. 4 shows the exchange of information over time between a Tag, Interrogator and the Application Processor using digital encryption techniques. The Interrogation of a Tag can be initiated merely by a Tag coming into Radio Frequency (RF) proximity of the Interrogator, depending on the exact service or specific application. In any case, the Tag senses the Interrogator's signal 401 and broadcasts its RFID 402. The Interrogator, which has no knowledge of the Tag's PIN or encryption key, sends the information along to the Application Processor, as identified by the type of ID number presented by the Tag. The Interrogator also generates a random number which it passes to both the Tag and Application Processor. The random number is chosen by the Interrogator 103 and is previously unknown to both the Tag and Application Processor. The Application Processor in turn looks up the appropriate identification information and, using the encryption information associated with the Tag's ID information, generates a response that is functionally based upon the RFID user's PIN (encryption key) and the random number sent by the Interrogator 405. Subsequently the Interrogator has also sent the same random number back to the Tag 404 and expects the same functionally based response 406. In this scenario, further transactions are allowed to continue between the Tag and Application Processor, through the Interrogator, only if the Processor and Tag return the same response to the random query. In this case, the Interrogator notifies the Tag and the Application Processor whether the transaction is accepted or rejected 409, 410. Note that in this scenario, no information about the Tag's PIN or encryption key has been transmitted anywhere in the network. The encryption key is only known by the Tag and Application Processor, which are distributed when the Tag is issued Also, all data is encrypted before transmission on any part of the network. The only information that is not protected is the Tag's ID number, which by itself is not useful to an eavesdropper and is treated as public information. Therefore, all three security issues outlined above are addressed by this method of user authentication and subsequent data transmission.

The security provided by the encryption method outlined here is that the response to the Interrogator's random number is based on a "one-way function" which produces the appropriate response. A one-way function is characterized by the fact that an eavesdropper that sees the output of the function cannot reconstruct the input (the secret PIN, in this case) even knowing the particular function. Both the Application Processor and the Tag use the same function, which is determined by the encryption key, to cipher and decipher the information data. FIG. 5a shows a Tag, using a one way function, calculating the response to a random query. In FIG. 5b, the "first round" of a DES encryption process is shown. In a DES level one code, there are 16 coding rounds to encrypt 64 bits of data. The exact function is unique to each user's database entry since it depends on the particular user's encryption key. For example, with today's technology, a 64 bit PIN can be encrypted using a DES level one function by a 8 bit microprocessor in approximately 1 ms. Thus it is a cost effective way to implement digital encryption and still be able to manufacture simple and cheap RFID Tags.

It is important to design system security that will be effective over the entire lifetime of the RFID system. As pointed out above, cellular network designers did not foresee the technical advancements and cost reductions of RF measurement equipment and the proliferation of cheap, powerful and portable computers. Therefore, one issue that must be addressed is what level of security can the MBS system provide against future attacks? Another implementation issue that will greatly effect the time response of the RFID system are the network and processing delays of the RF air interface and the connection to the authentication/transaction database.

Secure Messages

The previous example (FIG. 4) demonstrates how a Tag can exchange sensitive information with an Applica-

tion Processor. FIG. 6 shows how the Application Processor can change the information stored on a Read/Write RFID Tag. After the completion of the Tag authentication procedures described above, the Application Processor may find it necessary to change the information stored on the Tag. (For example, the remaining total on a debit card or the air waybill on an airline cargo container.) In this case the Application Processor will digitally encrypt all the command messages and information messages with the "encryption key" of the particular Tag. After completing all of the data transmission, the Tag will decrypt all of the new data and store it in memory. However, the RF channel is an unreliable medium and will generally create errors in the data transmission stream. Since only the endpoints of the network have the ability to decipher the information, unnecessary delay would be added if data, corrupted by wireless transmission, would need to be retransmitted between the endpoints. Since the Interrogator only has knowledge of the Tag's ID and not the PIN or encryption key, it needs a mechanism to ensure the Tag has received all the information correctly when transmitting over the radio channel.

Therefore, the Interrogator should add error detection and/or forward error correction coding to the transmitted data. This will allow any needed retransmissions to be only between the Tag and Interrogator, thereby reducing retransmission latency. For example, the Interrogator can calculate and add a CRC byte or bytes to the end of each transmitted packet, allowing both error detection and limited error correction. The Tag will in turn calculate the CRC for each received message packet and only ask for retransmission of corrupted packets.

Therefore, it is possible to send encrypted data between the Application Processor and a Tag without the need to pass encryption keys (PINs) over the wireless air interface. Since all data is encrypted before transmission to the Interrogator over the wired line, this method provides end-to-end security for the MBS system.

This leads to two immediate advantages: First, different applications can use different encryption algorithms, which can depend on the level of security the application needs or the maximum delay time an application can tolerate during information exchange. Since only the end points cipher, the data can be *a priori* encrypted and stored in memory thereby reducing latency. Second, as computers and microprocessors, the tools used by hostile eavesdroppers, become more powerful, the encryption algorithms can gracefully be updated by each generation release of the MBS system. Since only the Tag and the particular Application Processor entry for the Tag need to be updated, there is no need to modify any other parts of the MBS system.

Using the above techniques as an example, an inexpensive, short-range, bi-directional digitally encrypted radio communications channel is implemented. Implementation is made inexpensive by using, e.g., such Tag components as a Schottky diode, an amplifier to boost the signal strength, bit and flame synchronization circuits, an inexpensive 8-bit microprocessor, subcarrier generation circuits, and a battery. Most of these items are already manufactured in quantities of millions for other applications, and thus are not overly expensive.

The present invention outlines three levels of security for which, depending on the RFID application, an Application Processor, at least one Interrogator and at least one Tag can exchange information: The first level is the "Normal" mode, where a Tag and Interrogator exchange the RFID of the Tag. The second level is to transmit and detect a "secure" RFID between a Tag and Application Processor, using the Interrogator as a "wireless-to-wiredline" converter. The third level is the transfer of secure messages between a Tag and Application Processor. This can include downloading new information to a Tag; this is a "Read/Write" Tag where the data stored in memory is sensitive, such as cash stored on a debit card.

What has been described is merely illustrative of the application of the principles of the present invention. Other arrangements and methods can be implemented by those skilled in the art without departing from the spirit and scope of the present invention.

Claims

1. A radio communications system comprising a interrogator adapted to transmit radio signals, and at least one tag adapted to receive radio signals from the interrogator, wherein:

   the tag comprises a backscatter modulator in receiving relationship to a source of an encrypted signal, the backscatter modulator adapted to modulate reflections of radio signals from the interrogator using encrypted signals from said source, thereby to form at least one reflected modulated signal;
   the interrogator comprises a demodulator in receiving relationship to the reflected modulated signal, such that an encrypted signal is obtained by said demodulator; and
   the interrogator further comprises means for transmitting the encrypted signal to at least one application processor.

2. The radio communication system of claim 1, wherein:

   said at least one tag further includes a generator of a subcarrier signal, and a subcarrier modulator adapted to modulate the subcarrier signal using the encrypted signal; and
   the backscatter modulator is adapted to modu-

late radio-signal reflections using said subcarrier signal, thereby to form said reflected modulated signal.

3. The radio communications system of claim 1, further comprising at least one application processor, said processor comprising:

means for deciphering said encrypted signal, thereby to generate an information signal; and means for storing said information signal.

4. A radio communications system comprising an interrogator adapted to transmit radio signals, and at least one tag adapted to receive radio signals from the interrogator, wherein:

the tag comprises a backscatter modulator in receiving relationship to a source of a unique identifier, the backscatter modulator adapted to modulate reflections of radio signals from the interrogator using said unique identifier, thereby to form at least one reflected modulated signal;
the interrogator comprises a demodulator in receiving relationship to the reflected modulated signal, such that said unique identifier is recoverable from the reflected modulated signal;
the interrogator further comprises means for generating a random challenge and for transmitting the random challenge and the unique identifier to at least one application processor; and
the interrogator further comprises a modulator adapted to modulate the radio signals using the random challenge, and means for transmitting resulting modulated radio signals.

5. The radio communications system of claim 4, wherein:

said at least one application processor further includes means for generating a first encrypted response using a least said random challenge and using the unique identifier, and means for transmitting the first encrypted response to the interrogator;
said at least one tag further includes means for generating a second encrypted response using a least said random challenge, and backscatter modulation means for modulating the reflection of a radio signal using the second encrypted response, thereby to generate a modulated reflected signal; and
said interrogator further includes means for receiving the first encrypted response from at least one application processor, means for demodulating the modulated reflection signal to recover the second encrypted response, means for comparing the first and second encrypted responses, and means for accepting or rejecting results of such comparisons.

6. The radio communications system of claim 4 or claim 5, wherein:

said at least on tag further includes means for generating a subcarrier signal, and means for modulating the subcarrier signal using the unique identifier, thereby to form a modulated subcarrier; and
the backscatter modulator is adapted to modulate radio-signal reflections using the modulated subcarrier.

7. A radio communications system comprising an interrogator adapted to transmit radio signals, at least one tag adapted to receive radio signals from the interrogator, and an application processor, wherein:

the application processor comprises means for transmitting a encrypted information signal to the interrogator;
the interrogator is in receiving relationship to the application processor at least with respect to the encrypted information;
the interrogator comprises means for adding a unique identifier to at least one encrypted information signal received from the application processor, thereby to form a addressed information signal;
the interrogator further comprises means for adding cyclic redundant check coding to the addressed information signal, thereby to form a message signal;
the interrogator further comprises means for modulating a radio signal with the message signal, thereby to form a modulated radio signal, and means for transmitting the modulated radio signal to at least one tag;
the tag comprises means for receiving and demodulating the modulated radio signal, thereby to recover the message signal;
the tag further comprises means for calculating and removing the cyclic redundant check code from the message signal, thereby to recover the addressed information signal;
the tag further comprises means for removing the unique identifier from the addressed information signal, thereby to recover the encrypted information signal; and
the tag further comprises means for storing the encrypted information signal.

8. The radio communications system of claim 7, wherein the tag further comprises:

means for decrypting the encrypted information signal, thereby to recover unencrypted information; and
a storage medium for the unencrypted information.

9. The radio communications system of claim 7 wherein:

the tag further comprises means for determining the presence or absence of transmission errors based upon the cyclic redundant check coding, and means for generating a negative acknowledgment signal in the event of such transmission errors;
the tag further comprises a backscatter modulator adapted to modulate at least one reflection of a radio signal using the negative acknowledgment signal, thereby to form a backscatter-modulated signal;
the interrogator further comprises means for demodulating the backscatter-modulated signal, thereby to recover the negative acknowledgment signal;
the interrogator further comprises means for deciding, based on content of the negative acknowledgment signal, whether re-transmission should occur; and
the interrogator further comprises means for modulating a radio signal with the message signal, thereby to re-transmit the message signal.

10. A method of radio communication, comprising:

transmitting a radio signal from an interrogator to at least one tag;
in the tag, modulating the reflection of the radio signal using an encrypted signal, thereby forming a reflected modulated signal;
in the interrogator, receiving and demodulating the reflected modulated signal, thereby obtaining the encrypted signal; and
transmitting the encrypted signal to at least one application processor.

11. The method system of claim 10, further comprising:

in the tag, generating a subcarrier signal, and modulating the subcarrier signal using the encrypted signal; and wherein
the step of modulating the reflection of the radio signal is carried out using the subcarrier signal.

12. The method of claim 10, further comprising, in the application processor:

deciphering the encrypted signal, thereby to generate an information signal; and
storing the information signal.

13. A method of radio communication, comprising:

transmitting a radio signal from a interrogator to at least one tag;
in the tag, modulating a reflection of the radio signal using, at least in part, a unique identifier, thereby to form a reflected modulated signal;
in the interrogator, receiving and demodulating the reflected modulated signal, thereby to recover the unique identifier;
in the interrogator, generating a random challenge, and transmitting the random challenge and the unique identifier to a least one application processor; and
in the interrogator, modulating the radio signal using the random challenge, thereby to form a modulated radio signal, and transmitting the modulated radio signal.

14. The method of claim 13, further comprising:

in the application processor, generating a first encrypted response using a least said random challenge and the unique identifier;
transmitting the first encrypted response to the interrogator;
in the tag, generating a second encrypted response using a least said random challenge, and modulating the reflection of the radio signal using the second encrypted response, thereby to form the reflected modulated signal;
in the interrogator, receiving the first encrypted response from the application processor, demodulating the reflected modulated signal to recover the second encrypted response, and comparing the first and second encrypted responses; and
indicating acceptance or rejection of the result of the comparing step.

15. The method of claim 13 or claim 14, further comprising:

in the tag, generating a subcarrier signal, and modulating the subcarrier signal using the unique identifier, thereby to form a modulated subcarrier,
and in the tag, carrying out the step of modulating the radio-signal reflection by using the modulated subcarrier.

16. A method of radio communication, comprising:

transmitting an encrypted information signal from an application processor to an interrogator;
in the interrogator, adding a unique identifier to the encrypted information signal, thereby to form an addressed information signal;
adding cyclic redundant check coding to the addressed information signal, thereby to form a message signal;
modulating a radio signal with the message signal, thereby to form a modulated radio signal;
transmitting the modulated radio signal to at least one tag;
in the tag, demodulating the modulated radio signal, thereby to recover the message signal;
in the tag, calculating and removing the cyclic redundant check code from the message signal, thereby to recover the addressed information signal;
in the tag, removing the unique identifier from the addressed information signal, thereby to recover the encrypted information signal; and
in the tag, storing the encrypted information signal.

17. The method of claim 16, further comprising:

in the tag, decrypting the encrypted information signal, thereby to form unencrypted information, and storing the unencrypted information.

18. The method of claim 16, further comprising:

in the tag, determining the presence or absence of transmission errors based upon the cyclic redundant check coding, and generating a negative acknowledgment signal in the event of said transmission errors;
in the tag, modulating at least one reflection of a radio signal using the negative acknowledgment signal, thereby to form a backscatter-modulated signal;
in the interrogator, demodulating the backscatter-modulated signal, thereby to recover the negative acknowledgment signal;
deciding, based on the contents of the negative acknowledgment signal, whether re-transmission should occur; and
modulating a radio signal with the message signal, thereby to retransmit the message signal from the interrogator.

FIG. 1

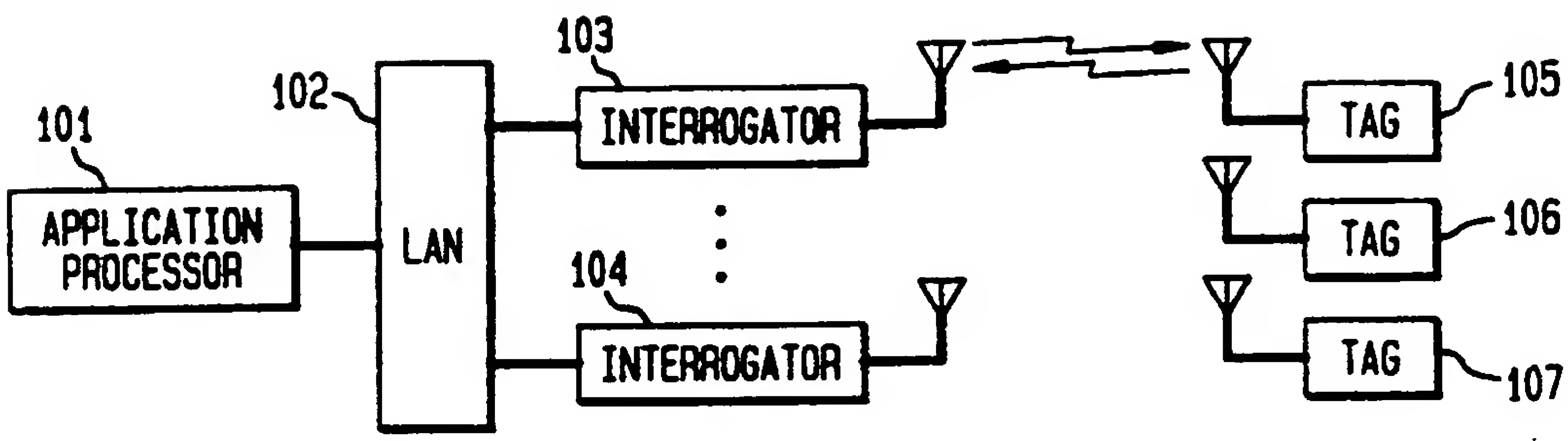

101
APPLICATION PROCESSOR
102
LAN
103
INTERROGATOR
104
INTERROGATOR
TAG
105
TAG
106
TAG
107

FIG. 2

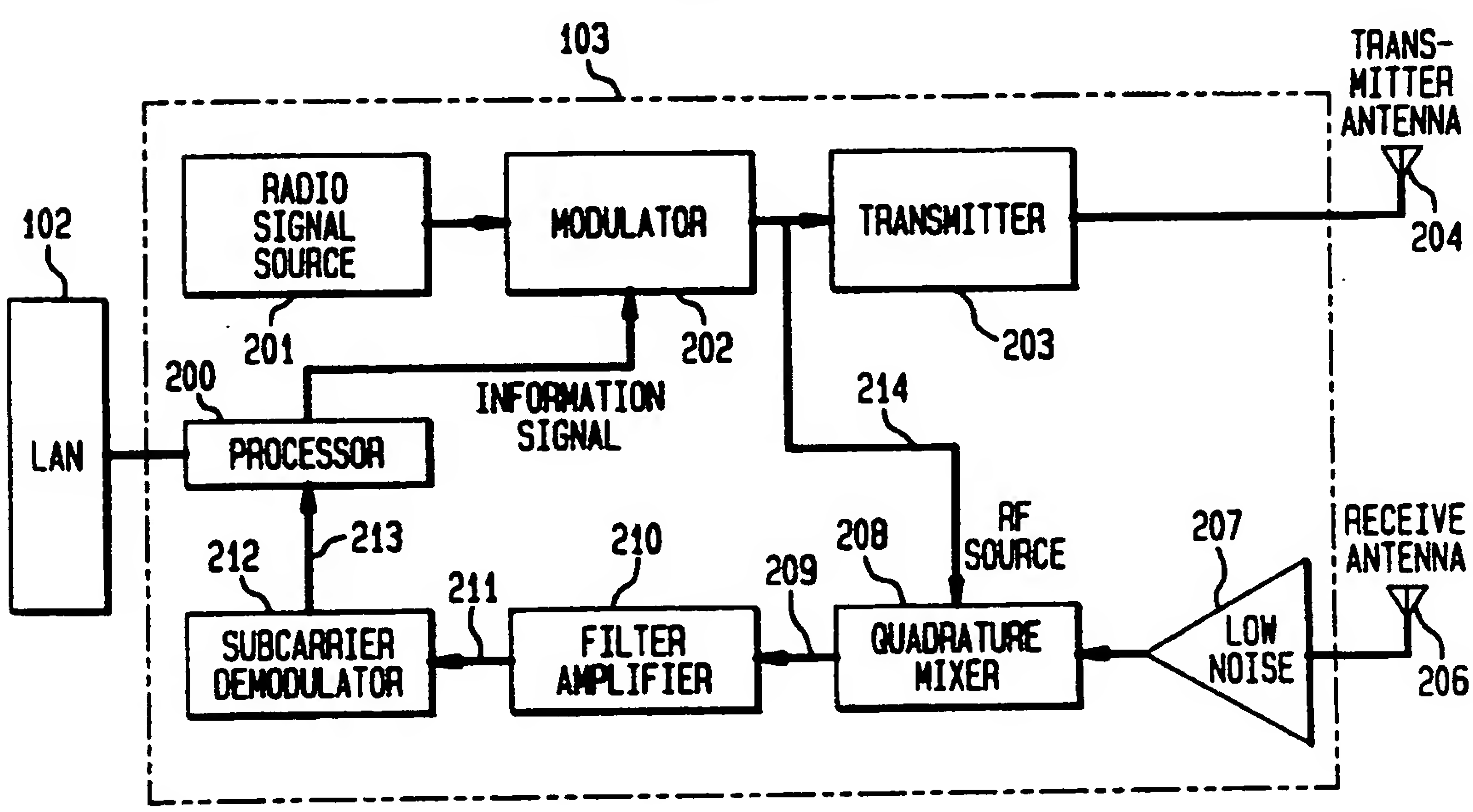

103
TRANS-MITTER ANTENNA
102
LAN
RADIO SIGNAL SOURCE
MODULATOR
TRANSMITTER
204
201
202
203
200
PROCESSOR
INFORMATION SIGNAL
214
RF SOURCE
212
213
210
211
209
208
207
RECEIVE ANTENNA
SUBCARRIER DEMODULATOR
FILTER AMPLIFIER
QUADRATURE MIXER
LOW NOISE
206

FIG. 3

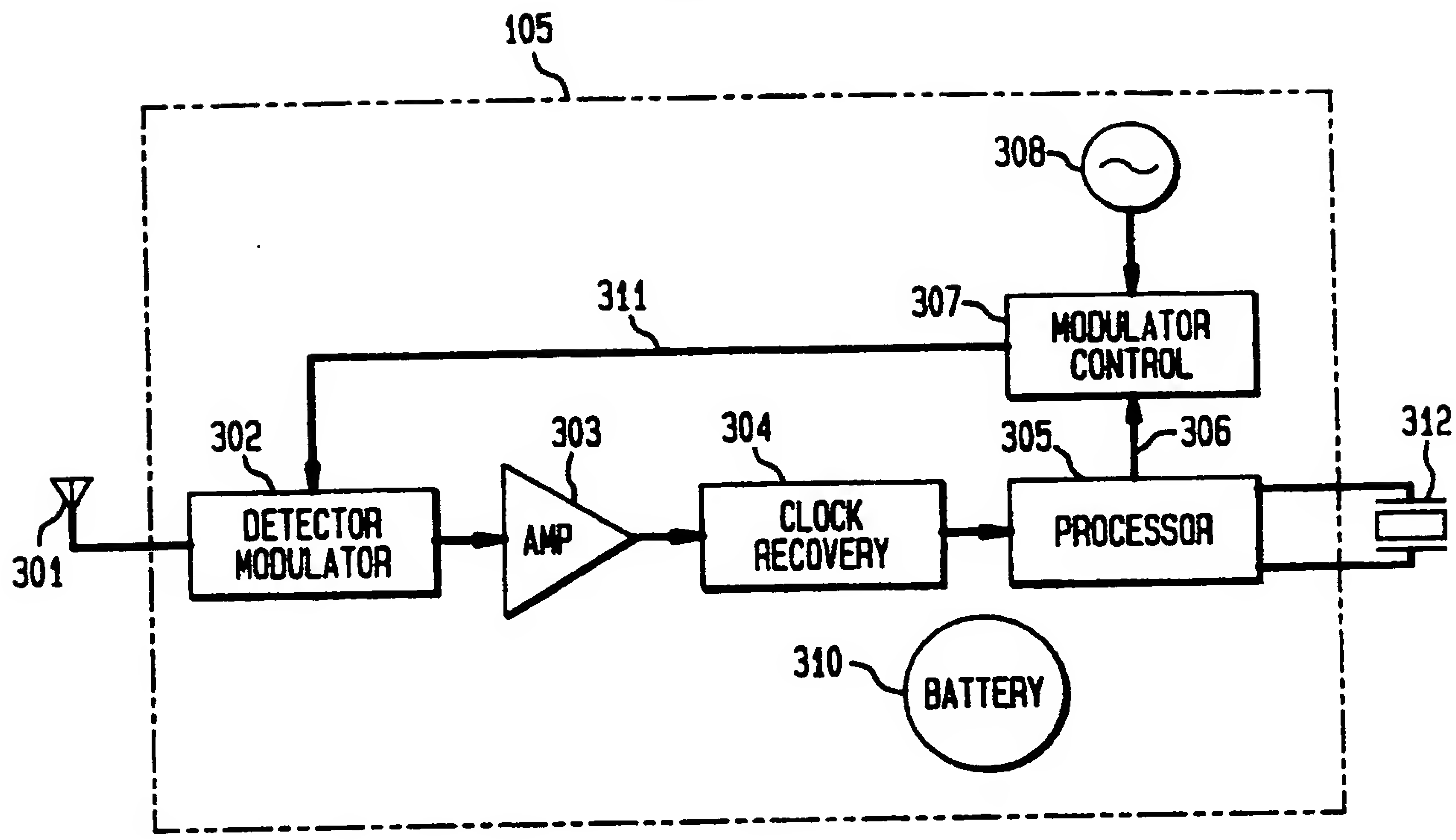

105
308
311
307
MODULATOR CONTROL
302
303
304
305
306
312
301
DETECTOR MODULATOR
AMP
CLOCK RECOVERY
PROCESSOR
310
BATTERY

FIG. 4

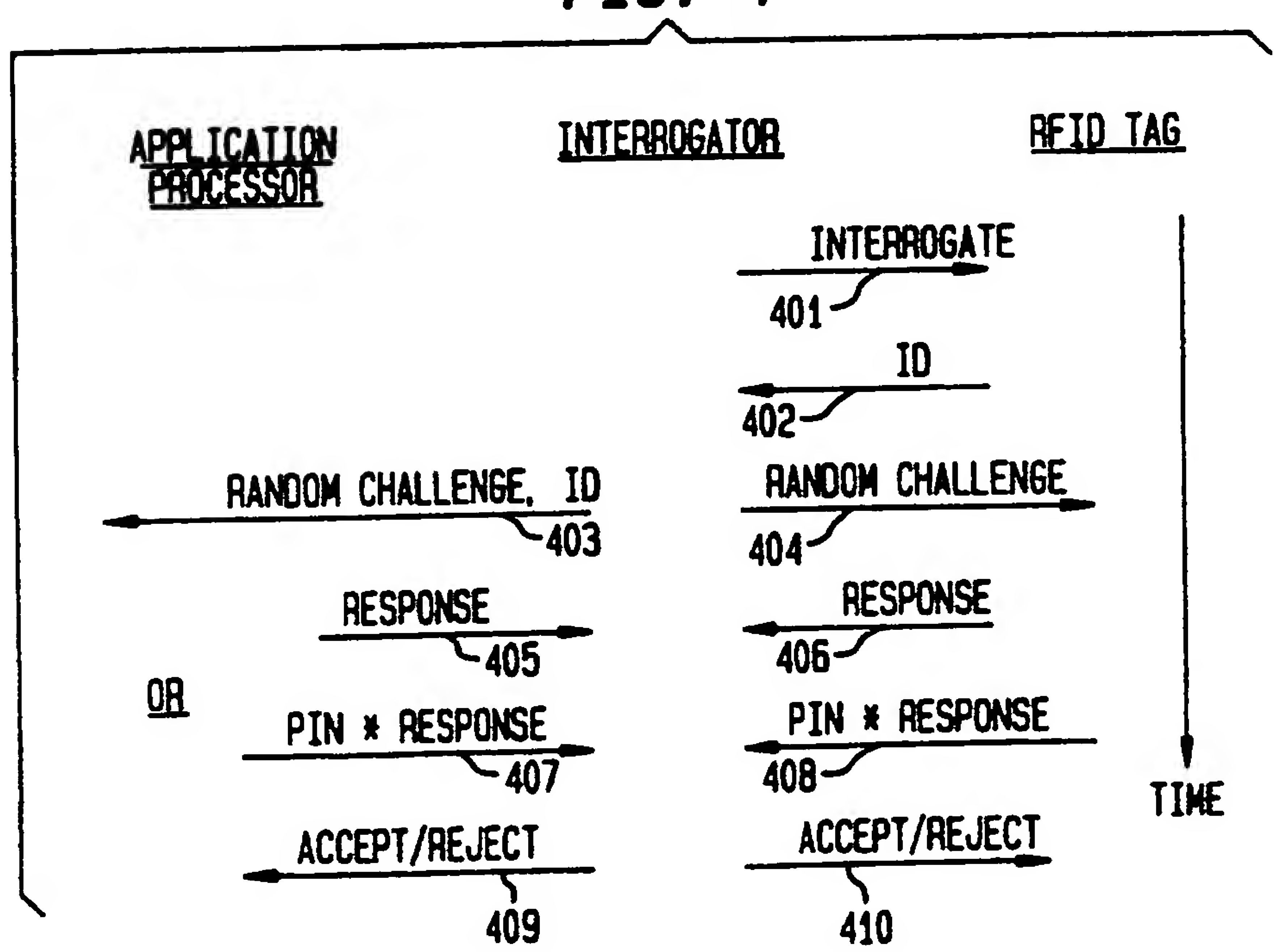

APPLICATION PROCESSOR
INTERROGATOR
RFID TAG
INTERROGATE
401
ID
402
RANDOM CHALLENGE, ID
403
RANDOM CHALLENGE
404
RESPONSE
405
RESPONSE
406
OR
PIN * RESPONSE
407
PIN * RESPONSE
408
TIME
ACCEPT/REJECT
409
ACCEPT/REJECT
410

FIG. 5A

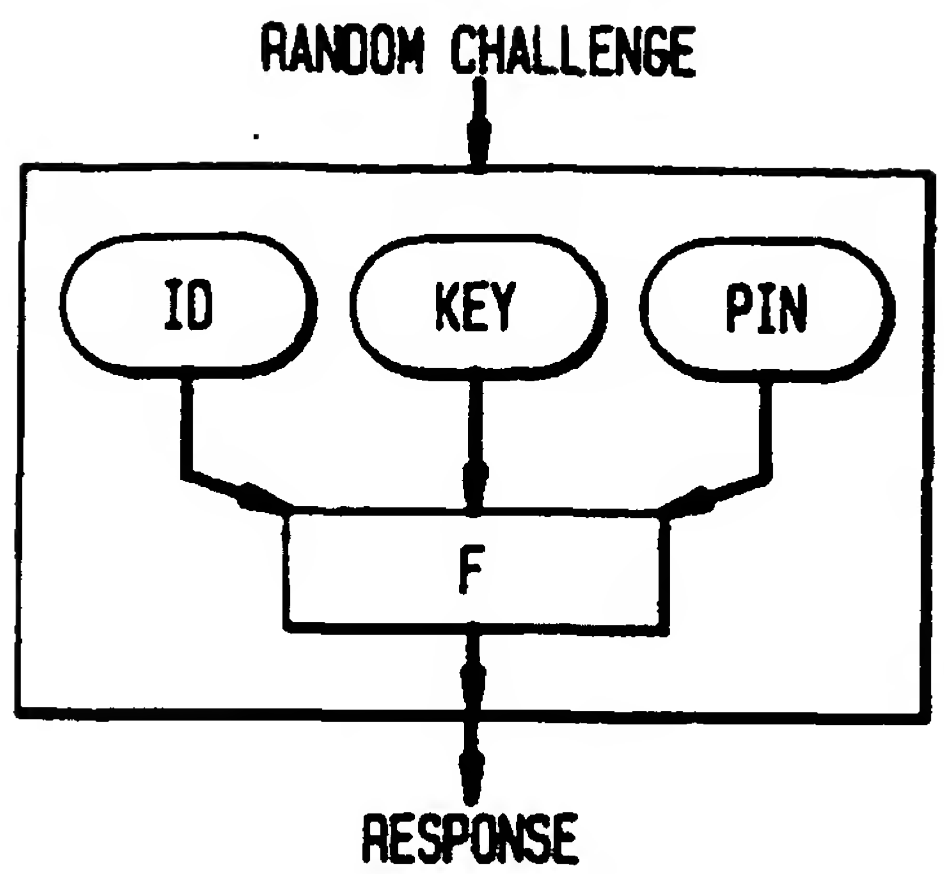


FIG. 5B

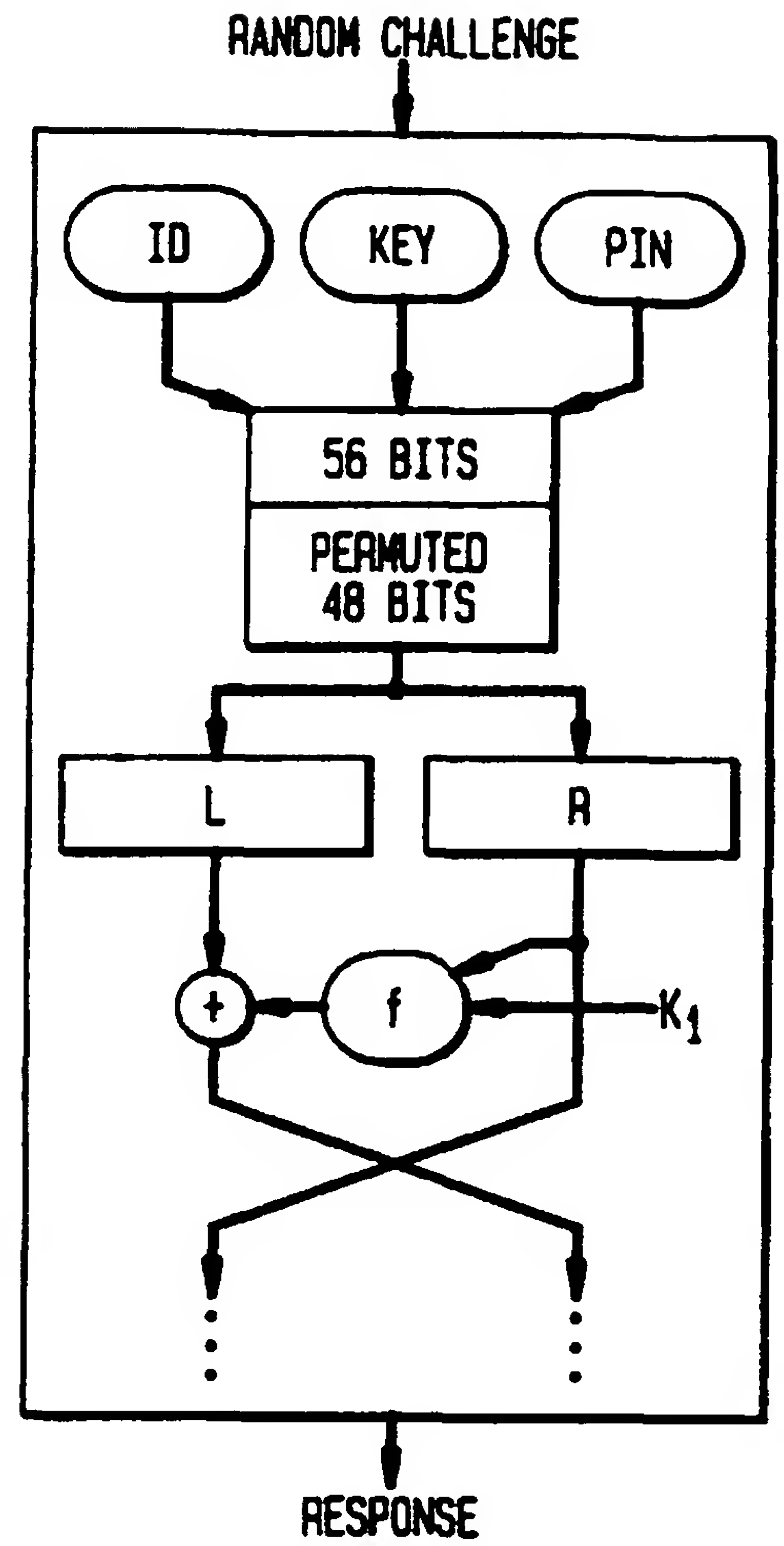


FIG. 6